SOME THEOREMS ON PERMUTATION POLYNOMIALS[1]

BY L. CARLITZ

Communicated by G. B. Huff, December 8, 1961

A polynomial $f(x)$ with coefficients in the finite field $GF(q)$ is called a permutation polynomial if the numbers $f(a)$, where $a \in GF(q)$ are a permutation of the a's. An equivalent statement is that the equation

$$f(x) = a \tag{1}$$

is solvable in $GF(q)$ for every a in $GF(q)$. A number of classes of permutation polynomials have been given by Dickson [1]; see also Rédei [3].

In the present note we construct some permutation polynomials that seem to be new. Let $q = 2m+1$ and put

$$f(x) = x^{m+1} + ax. \tag{2}$$

We define

$$\psi(x) = x^m, \tag{3}$$

so that $\psi(x) = -1, +1$ or 0 according as x is a nonzero square, a nonsquare or zero in $GF(q)$. Thus (2) may be written as

$$f(x) = x(a + \psi(x)). \tag{4}$$

We shall show that for proper choice of a, the polynomial $f(x)$ is a permutation polynomial. We assume that $a^2 \neq 1$; then $x = 0$ is the only solution in the field of the equation $f(x) = 0$. Now suppose (i) $f(x) = f(y)$, $\psi(x) = \psi(y)$. It follows at once from (4) that $x = y$. Next suppose (ii) $f(x) = f(y)$, $\psi(x) = -\psi(y)$. Then (4) implies

$$\psi\left(\frac{a+1}{a-1}\right) = -1. \tag{5}$$

If we take

$$a = \frac{c^2+1}{c^2-1}, \tag{6}$$

where $c^2 \neq \pm 1$ or 0 but otherwise is an arbitrary square of the field, it is evident that (5) is not satisfied. For $q \geqq 7$ such a choice of c^2 is

[1] Supported in part by National Science Foundation grant G-16485.